DATE(S) ISSUED:

06/10/2014

SUBJECT:

Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (MS14-036)

EXECUTIVE SUMMARY:

Two vulnerabilities have been discovered in the Microsoft Graphics component that could allow remote code execution in Microsoft Windows, Microsoft Office, and Microsoft Lync. Microsoft Windows is a popular operating system for both workstations and servers. Microsoft Office is an office suite of desktop applications. Microsoft Lync is a unified communications platform.

Successful exploitation of these vulnerabilities could result in an attacker taking complete control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

These vulnerabilities are not publicly disclosed and there are no open source reports that they are currently being exploited in the wild.

SYSTEM AFFECTED:

- · Windows Server 2003
- · Windows Vista
- · Windows Server 2008
- · Windows Server 2008 R2
- · Windows 7
- · Windows 8 and 8.1
- · Windows Server 2012
- · Windows Server 2012 R2
- · Windows RT
- · Windows RT 8.1
- · Microsoft Office 2007
- · Microsoft Office 2010
- · Microsoft Live Meeting 2007
- · Microsoft Lync 2010

· Microsoft Lync 2013

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Two vulnerabilities have been discovered in MicrosoftGraphics Component, which could allow an attacker to take complete control of an affected system. These vulnerabilities could allow an attacker to execute remote code by luring a victim to a malicious website or to accept a shared document file specially crafted to exploit these vulnerabilities.

· ***Unicode Scripts Processor Vulnerability (CVE-2014-1817):*** A remote code execution vulnerability exists in the way that affected components handle specially crafted font files. The vulnerability is caused when Windows fails to properly handle specially crafted files in a way that corrupts memory and allows for arbitrary code to be executed. The Unicode Script Processor (usp10.dll), also known as Uniscribe, is a collection of APIs that enables a text layout client to format complex scripts. Uniscribe supports the complex rules found in scripts such as Arabic, Indian, and Thai. Uniscribe also handles scripts written from right-to-left such as Arabic or Hebrew, and supports the mixing of scripts. For plain-text clients, Uniscribe provides a range of ScriptString functions that are similar to TextOut, with additional support for caret placement. The remainder of the Uniscribe interfaces provides finer control to clients.

· ***GDI+ Image Parsing Vulnerability (CVE-2014-1818):*** A remote code execution vulnerability exists in the way that GDI+ handles validation of specially crafted images. The vulnerability is caused when GDI+ improperly validates specially crafted image files. GDI+ is a graphics device interface that provides two-dimensional vector graphics, imaging, and typography to applications and programmers.

Successful exploitation of these vulnerabilities could result in an attacker taking complete control of the system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- · Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- · Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- · Remind users not to click links from unknown sources, or to click links without verifying the intended destination.
- · Do not open email attachments from unknown or untrusted sources
- · Consider implementing file extension whitelists for allowed e-mail attachments

REFERENCES:

Microsoft:

https://support.microsoft.com/kb/2967487

https://technet.microsoft.com/library/security/ms14-036

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1817

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1818